File SAFE

CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

SAF-E434-81
24 June 1981

Mr. Robert D. Williams
Building E1
Room 5076

Subject   :   Addressing of Key Issues

Dear Mr. Williams,

As we together follow up on the results of PDR and the subsequent TRW audit of the project, there are a number of key issues which need to be addressed if we are to avoid revisiting slipping schedules and uncertain technical progress. Most have been addressed orally over a period of time with varied results. I will attempt to state them concisely and provide you with the Government's perception.

1.   Software Design - The overall structure of the system software has not been defined since the System Design Specification and that definition is both dated and at a low level of resolution. The system services "layer" in particular with its attendant control mechanisms has been elusive. The interfaces among software entities and indeed the entities themselves have not been well defined.

It appears that only in attempting to build prototype software did the designers realize that the "finite state machine" model would not perform effectively. This gives rise to the question, "was (or will) the design be carried out to a level required for analysis to predict problems before they are enountered by coders?" The Process Design Document is now supposed to define the software structure. It must - and soon. It seems impossible that any real progress can be made on DMS or the application layer until the system services layer is structurally defined.

There is danger that "prototype" code developed early will fill the void in the design and an ill-designed system will result. Continual Government criticism of the (high overhead) scheme outlined in reviews from November 1980 to May 1981 had absolutely no effect. Only by pursuing the process to coding did TRW become aware that it was unworkable and it appears that 6 months has been wasted.

The lack of design documentation prevented, to a degree, criticism and proper follow-up. The Government will seek ways to be more effective in providing positive criticism in the future.

2. Software Development Management - A number of problems in the software status are traceable to the management of that effort.

   a) The senior designers were removed from the project before the design was taken to a level of detail to permit evaluation of its merit.

   b) Very intelligent but less experienced designers took over and followed a (promising) theoretical approach too far before discovering basic problems.

   c) The software design was "farmed out" to various development groups in spite of the lack of overall structural definition. Lack of progress in these groups is to be expected.

   d) Current assurances that we can recover schedule are based on the premise that we are on course but behind. The course is not clear to the Government.

   e) The software, if not brought under strong technical management control at once, is going to become a disaster.

   f) Current management in that area is inadequate at the top. Band-aid solutions such as sharp consultants are not adequate. Some extremely impressive talent is obvious in the group but the structure and the management are wrong. The situation requires the insertion of strong, senior software development management. It can augment or replace current management but the organization must be aligned to the tasks at hand.

There is an impressive array of talent assigned to the program. Middle level managers appear effective but the basic system design problems prevented progress and top managers have not taken effective action to resolve basic problems. The block orientation was the most effective course at the time it was initiated, but simply dropping all unfinished business on the Block Czars because System Engineering was not able to carry on the design was an abdication of responsibility by higher management.

3. Planning - High level plans are well done. They are lucid and thorough. Reduction to lower levels seems to be weak with a lack of rigor which throws into question the validity of the top level plans. At best it makes tracking of progress against plan and the assessment of impact of a missed event almost impossible. The constancy of the replanning effort can be traced in large measure to the failure to execute earlier plans. Earned value appears to have the same function and value as an autopsy. In a program as complex as SAFE, only a network planning approach (PERT, CPM) at a high level of detail provides an adequate mechanism to ensure integrity and measurement of progress against plan.

4. Organization and Management - All software development (except WBCS) falls in the Sub-System Development group. The design approach (Finite State Machine) is broken and the re-design seems to fall upon the "Block Czars." Both are impressive as results-oriented managers, but are unknown quantities as large-scale software system designers. The software "engineers" re-designing the system mechanics are the same ones who designed the last one - extremely bright but not seasoned. The situation cries out for a (small) team of senior designers to reconstruct a minimum-breakage course to a software design which can be built according to our recently-discussed plans. As a minimum, a senior oversight mechanism should oversee the technical work.

Further, when a program is in trouble it is generally advantageous to provide close proximity to groups working on common tasks and to avoid disruptions of work routine. The necessity for splitting the technical developers into three buildings, with attendant moves,

at a critical juncture in the design process while keeping other programs in building 103, (especially after SAFE staffing was 80% complete in 103) was never explained. "They don't fit anyway" was not considered adequate as long as other projects and administrative functions remained in 103.

Top management of Sub-System Development is not effective in this activity. Introduction of transients is hazardous but clearly the present course is fraught with peril. A great deal of visibility will be asked by the Government in this area and TRW should oversee it very carefully.

5. Preliminary Design Review - This activity must be adjudged unsuccessful in that it did not review the software design. The expectation was that the software architecture and the structure down to the unit level would be reviewed at least for Block 1. In spite of the results of PDR we agreed, after providing TRW with a candid critique and receiving assurances that follow-up action would be reported to the Government, that we must press on. A technical audit was conducted by TRW and a number of actions were initiated to correct deficiencies. A Process Design Document was to capture the software design. That document is late and the outline is not clear as to the degree to which the system design - particularly for Block 1 - will be defined. There seems to be no differentiation for example between "system software" and "application software" - a differentiation which must be made and retained if the system is to be useful over a long period of time.

PDR then consisted primarily of form to pass a "milestone" but as for software, the substance was missing. The Process Design Document must be reviewed carefully as to scope and content if it is to be the definition of the software architecture.

While the foregoing is somewhat disjoint, it does reflect my major concerns and should indicate why my confidence in the success of near-term technical developments is shaken. The

—4—

relative ease with which we have each accommodated to changes
in plans reflects, in addition to a mutual willingness to solve
problems, a lack of rigor in the planning process. In particular
definitions of milestones and dependencies among events has been
so loose as to permit ad hoc activities and substantial changes
to occur without an obvious impact on the program.

As we move forward on our replanned course to IOC, we
will be especially interested in results - in the form of designs,
code, functions and all it takes to make SAFE go. I hope that
our discussions over the past several months and the concerns
outlined are helpful in your oversight of the program. I plan
to review them regularly to re-establish confidence in the
outcome.

I would be happy to discuss any aspects of the program
at greater length if it would be helpful.

STAT

Sincerely,

Director, Consolidated SAFE
Project Office/ODP

-5-